TAMPEREEN
AMMATTIKORKEAKOULU

WLAN-VERKKOSUUNNITELMAN LAATIMINEN PROAKATEMIALLE

Ari-Matias Angeria

Opinnäytetyö
Marraskuu 2015
Tietojenkäsittelyn koulutusohjelma
Tietoverkkopalvelut

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Tietoverkkopalvelut

ANGERIA, ARI-MATIAS:
WLAN-verkkosuunnitelman laatiminen Proakatemialle

Opinnäytetyö 28 sivua
Marraskuu 2015

Opinnäytetyön tavoitteena oli kartoittaa langattomien lähiverkko- eli WLAN-yhteyksien toimintaa Tampereen ammattikorkeakoulun yrittäjyyden yksikön, Proakatemian, uusissa toimitiloissa. Tavoitteena oli myös tutkia langattoman lähiverkon toimintaa sekä teoriassa että käytännössä uudella kampusalueella. Proakatemian tilojen verkkoympäristöön kuuluu lukuisia langatonta verkkotekniikkaa hyödyntäviä laitteita, joten langattoman verkon tulee toimia luotettavasti uudessa toimipisteessä.

Opinnäytetyön tarkoituksena oli parantaa WLAN-verkon toimintaa Proakatemian uudella kampusalueella, joten opinnäytetyön päämenetelmäksi valittiin langattoman lähiverkon kantavuuden mittaaminen. Uuden kampusalueen WLAN-verkko mitattiin kannettavan tietokoneen ja verkonsuunnitteluun ja -kartoitukseen soveltuvan Ekahau HeatMapper -ohjelman avulla. Mittaukset toteutettiin itsenäisesti elokuussa 2015.

Mittaustuloksista ja suunnitelmasta laadittu yhteenveto välitettiin TAMKin kampusten verkoista vastaavalle tietohallinnolle. Tietohallinnolta saadun palautteen perusteella sekä mittaustuloksiin että verkon kehittämissuunnitelmaan tehtiin täsmennyksiä ja kehitysehdotuksia. Tässä opinnäytetyössä esitellyt mittaustulokset ja verkonkehityssuunnitelma jäävät TAMKin tietohallinnon käyttöön Proakatemian verkon parantamiseen.

Verkkomittausten ohella opinnäytetyössä tutkittiin langattomien lähiverkkojen historiaa, salausmenetelmiä ja tietoturvauhkia aiheeseen liittyvän kirjallisuuden ja verkkolähteiden lähteiden avulla.

Asiasanat: langaton lähiverkko, verkon kuvaus, verkon mittaus, WLAN

ABSTRACT

Tampere University of Applied Sciences
Degree Programme in Business Information Systems
Network Services

ANGERIA, ARI-MATIAS:
WLAN Network Plan for Proacademy

Bachelor's thesis 28 pages
November 2015

This thesis was commissioned by Proacademy in Tampere University of Applied Sciences. The main goal was to map the overall situation of the wireless local area network environment at the new Proacademy campus. Computers, mobile phones and other electronic devices use WLAN connections nowadays, which is why the wireless network must be a functioning and reliable option for networking.

The main purpose of this thesis was to measure the carrying capacity of the WLAN network which was put into practice using Ekahau HeatMapper network planning software. The research results were presented to the IT administration of TAMK after the results were analyzed, opened up and summarized. According to the results wireless access points may be placed differently to improve the network performance at the campus area.

Besides reporting the measuring and analysis of the wireless local area network at Proacademy, this thesis contains general information about WLAN networks and its technologies, encryption methods and security threats towards WLAN networks.

Key words: network analysis, network mapping, wireless local area network, WLAN

SISÄLLYS

LYHENTEET JA TERMIT

802.11	IEEE:n määrittelemä langattoman lähiverkon standardi
AES	*Advanced Encryption Standard* – Vahva salausmenetelmä
BSS	*Basic Service Set* – Tukiasemaan perustuva verkkotopologia
BYOD	*Bring Your Own Device* – Henkilökohtaisten tietoteknisten ja mobiililaitteiden käyttäminen töissä ja opinnoissa
DDoS	*Distributed Denial of Service* – Hajautettu palvelunestohyökkäys
DoS	*Denial of Service* – Palvelunestohyökkäys
DS	*Distribution System* – ESS-verkkotopologian runkoverkko
ESS	*Extended Service Set* – Laajennettu tukiasemaan perustuva verkkotopologia
FCC	*Federal Communications Commission* – Yhdysvaltain telehallintovirasto
IBBS	*Independent Basic Service Set* – Vertaisverkkoon perustuva verkkotopologia
IEEE	*Institute of Electrical and Electronics Engineers* – Suuri kansainvälinen tekniikan alan järjestö
ISM	*Industrial, scientific and medical radio band* – Maailmanlaajuinen, vapaasti käytettävä radiotaajuusalue; käytössä esimerkiksi Bluetooth- ja WLAN-yhteyksissä
Mbit/s	Tiedon siirtymisen nopeus, joka mitataan megabittiä sekunnissa
MIMO	*Multiple-input, multiple-output* – Useamman antennin hyödyntäminen langattomassa verkkoliikenteessä
RADIUS	*Remote Authentication Dial-In User Service* – Kaksisuuntainen todennustapa laitteen ja verkon välillä
SSID	*Service Set Identifier* – Langattoman lähiverkon yksilöivä verkkotunnus
TKIP	*Temporal Key Integrity Protocol* – Langattomien lähiverkkojen tietoturvaprotokolla, joka huolehtii yhteyksien salaamisesta ja turvaamisesta

verkkotopologia	Tietokoneverkon perusrakenne, joka osoittaa, kuinka verkon laitteet on liitetty toisiinsa
VPN	*Virtual Private Network* – Virtuaaliverkkoyhteys, jonka avulla voidaan muodostaa suojattu yhteys salaamattoman verkon yli
WEP	*Wired Equivalent Privacy* – Langattoman verkon varhaisin salausmenetelmä
WLAN	*Wireless Local Area Network* – Langaton lähiverkko
WPA	*Wi-Fi Protected Access* – WEP-salausmenetelmän seuraaja
WPA2	WPA-salausmenetelmän päivitetty versio

1 JOHDANTO

Tämä opinnäytetyö käsittelee langattoman lähiverkon toimintaa Tampereen ammattikorkeakoulun yrittäjyyden yksikön, Proakatemian, uusissa toimitiloissa. TAMKin opiskeluyksikön Proakatemian verkkoympäristön käyttäjäjoukko koostuu TAMKin opettajista ja oppilaista sekä vierailijoista, joten etenkin langattoman WLAN-verkon tulee toimia vakaasti ja kattavasti koko kampusalueella.

TAMKin Proakatemian uusissa toimitiloissa opiskelee liiketalouden ja tietojenkäsittelyn opiskelijoita, jotka perustavat oman tiimiyrityksen ja vastaavat sen toiminnasta. Proakatemian koulutusohjelma perustuukin yritystoiminnan kautta tapahtuvaan osallistavaan toimintatapaan, joka on huomioitu myös Proakatemian tilojen suunnittelussa. (Proakatemia.fi 2015.) Suurien luokkahuoneiden sijaan toimitilat koostuvat neuvottelu-, paja- ja taukotiloista.

Opinnäytetyön tarkoituksena on parantaa WLAN-verkon toimintaa Proakatemian uudella kampusalueella, joten opinnäytetyön päämenetelmänä on langattoman lähiverkon kantavuuden mittaaminen. Uuden kampusalueen WLAN-verkon mittauksessa käytetään kannettavaa tietokonetta ja verkonsuunnitteluun ja -kartoitukseen soveltuvaa Ekahau HeatMapper -ohjelmaa. Opinnäytetyön toisessa luvussa tarkastellaan langattomien lähiverkkojen historiaa, topologioita ja tietoturvaa. Työn kolmannessa luvussa kartoitetaan Proakatemian verkkoympäristöä ja sen käyttäjiä sekä verkon vaatimuksia. Neljäs luku sisältää Proakatemian WLAN-verkon mittaamisen lähtökohtia, mittaustuloksia ja niiden analysointia sekä parannusehdotuksia.

TAMKin tietohallinnolta saadun palautteen perusteella sekä mittaustuloksiin että verkon kehittämissuunnitelmaan tehdään täsmennyksiä ja kehitysehdotuksia, jonka jälkeen mittaustuloksista laaditaan lopullinen yhteenveto ja toimitetaan se TAMKin tietohallinnolle. Näin tässä opinnäytetyössä esitellyt mittaustulokset ja verkonkehityssuunnitelma jäävät TAMKin tietohallinnon hyödynnettäväksi Proakatemian verkkoa parannettaessa.

2 LANGATON LÄHIVERKKO

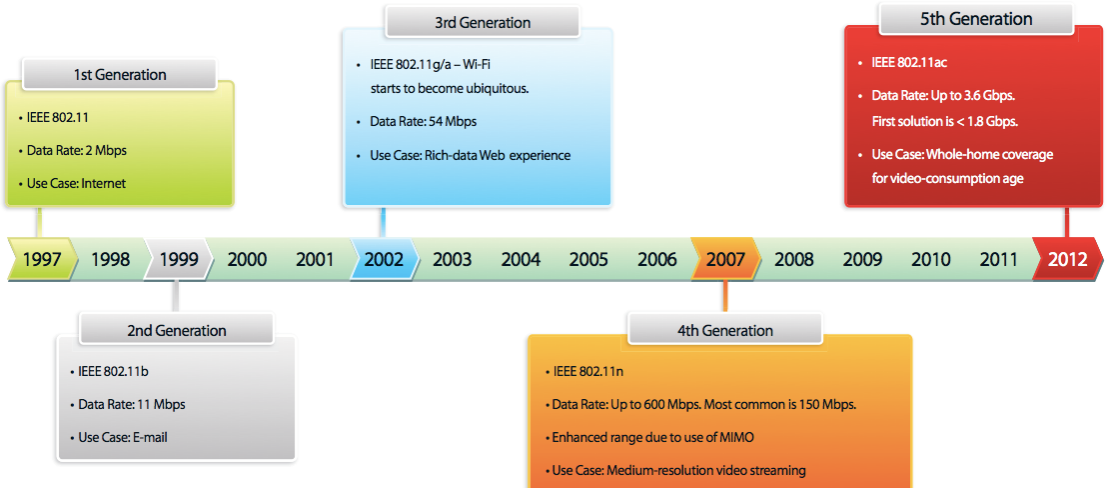
2.1 Langattoman lähiverkon historiaa

Langattomien lähiverkkojen alkutaival sijoittuu 1980-luvun puoliväliin, jolloin Yhdysvaltain telehallintovirasto FCC (Federal Communications Commission) vapautti teolliseen ja tieteelliseen käyttöön tarkoitetun ISM-taajuusalueen vapaaseen käyttöön (Ahonen 2014). Vuonna 1990 Motorola toi markkinoille ensimmäisen merkittävänä langatonta lähiverkkotekniikkaa hyödyntävän Altairin (kuva 1).

KUVA 1. Motorola Altair (Computer History Museum 2015).

Kansainvälinen tekniikan alan järjestö Institute of Electrical and Electronics Engineers (IEEE) perusti LAN/MAN-komitean (IEEE 802 LAN/MAN Standards Committee), joka aloitti langattoman lähiverkon standardikehityksen vuonna 1990. Komitean muutaman vuoden kehitystyön tuloksena julkaistiin ensimmäinen 802.11-standardi vuonna 1997, jonka nopeus oli maksimissaankin vain 2 megabittiä sekunnissa. Ensimmäisen 802.11-standardin jälkeen uusia WLAN-standardeja on ilmestynyt aina muutaman vuoden välein. (Puska 2005, 15.) 802.11a-, 802.11b- ja 802.11g-standardien myötä langat-

tomat verkkotekniikat ovat tulleet entistä nopeammiksi, turvallisemmiksi ja luotettavammiksi ja WLAN-standardit kehittyvät yhä (kuva 2).



KUVA 2. Merkittävimmät IEEE 802.11-standardit aikajärjestyksessä (Shimpi 2012).

Vuonna 2009 IEEE hyväksyi langattomille lähiverkoille 802.11n-standardin, joka parantaa aiempien standardien suorituskykyä teoriassa jopa 600 megabittiin sekunnissa (Puustinen 2009). 802.11n-standardi on myös laatuaan ensimmäinen, joka tukee niin sanottua MIMO-tekniikkaa (multiple-input, multiple-output), jossa käytetään lähetettävään ja vastaanotettavaan signaaliin useampaa antennia. Niin sanotun moniantennitekniikan avulla saadaan parannettua sekä tiedonsiirtonopeuksia että tiedonsiirron luotettavuutta. (Puska 2005, 127.)

Uusin WLAN-standardi 802.11ac esiteltiin vuonna 2011 ja se moninkertaistaa langattoman lähiverkon tiedonsiirtonopeudet megabiteistä gigabitteihin. Teoriassa suurin tiedonsiirtonopeus 802.11ac-verkossa on 600 megabittiä sekunnissa, mutta todennäköistä kuitenkin on, että käytännössä tiedonsiirtonopeus kasvaa korkeintaan kolmin- tai nelinkertaiseksi aiempaan 802.11n-standardiin verrattuna. (Mäkinen 2012.) IEEE hyväksyi kolmen vuoden kehitystyön jälkeen 802.11ac-standardin vuonna 2014, minkä lisäksi kehitteillä on muun muassa jopa sadan gigabitin siirtonopeuteen yltävä 802.11ay-standardi (Kelly 2014).

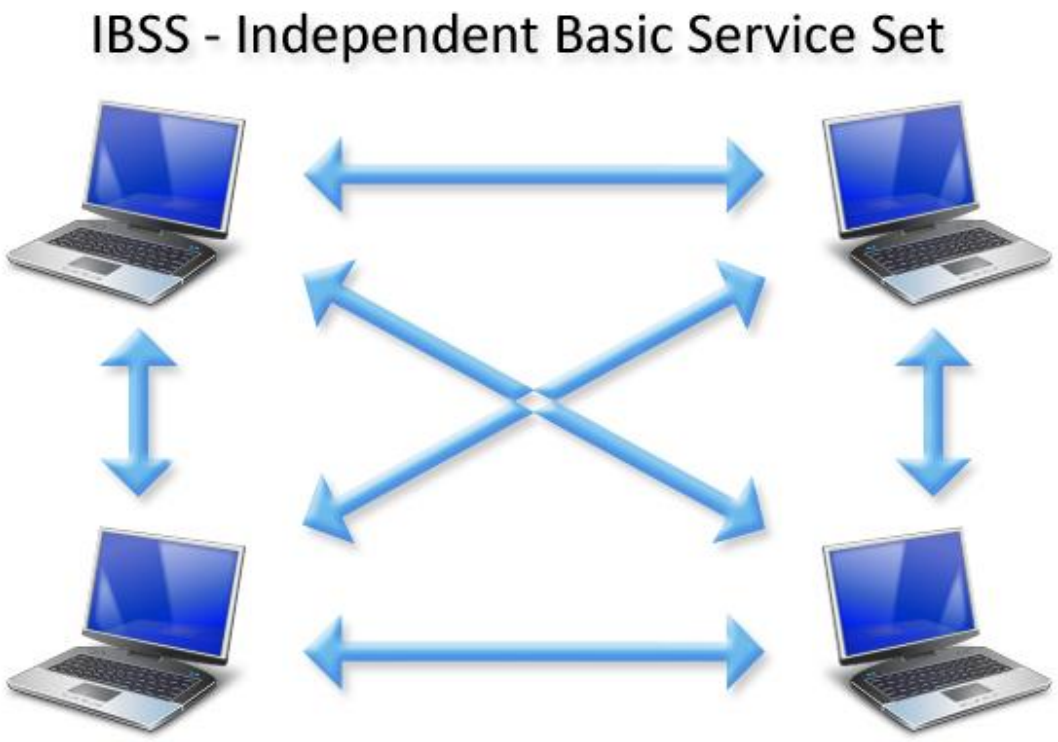
WLAN-standardien kehityksen myötä langattomien verkkojen suosio on kasvanut huimasti yksityishenkilöiden ja yritysten käytössä. Langattoman verkon mahdollisuudet ovat rajattomat ja tilapäisten verkkoympäristöjen rakentaminen onnistuu nopeasti ilman kaapelointia. (Puska 2005, 13.)

2.2 Langattoman lähiverkon topologiat

IEEE 802.11-standardi määrittelee kaksi erilaista topologiaa: vertaisverkkoon perustuva topologia ja tukiasemaan perustuvan topologian. Näiden topologioiden eroavaisuuksia käsitellään seuraavissa alaluvuissa.

2.2.1 Vertaisverkkoon perustuva topologia

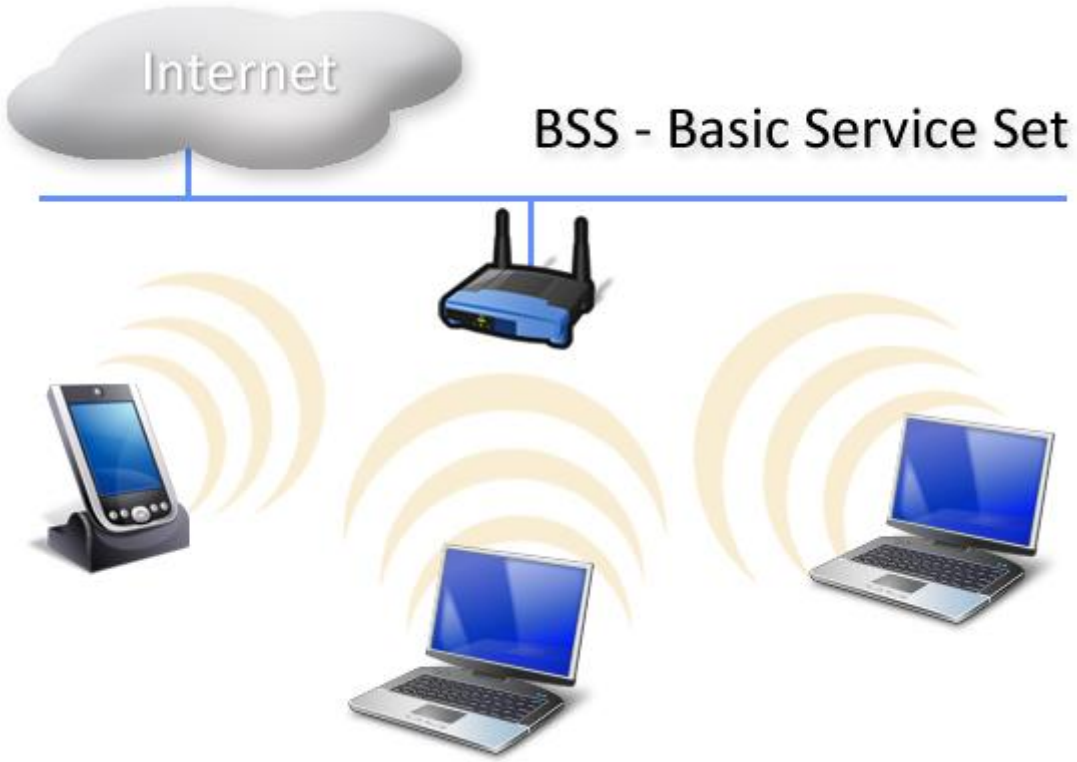
Vertaisverkkoon perustuvasta mallista käytetään nimitystä IBSS (Independent BSS) (kuva 3), jossa laitteiden muodostama verkko ei kytkeydy kiinteään verkkoon, vaan kaikki laitteet "keskustelevat" suoraan toistensa kanssa. IBSS-verkkoa voidaan tarvita esimerkiksi tilanteessa, kun tiedostoja ja tulostimia tulisi jakaa useamman tietokoneen käyttöön, mutta käytettävissä ei ole tukiasemaa. IBSS-verkko on kuitenkin yleensä lyhytikäinen ratkaisu, sillä IBSS-verkon tietokoneita ei voida kytkeä samanaikaisesti muihin verkkoihin. (Granlund 2007, 294–295.)



KUVA 3. Vertaisverkkoon perustuva verkkotopologia (Jumpluf 2014).

2.2.2 Tukiasemaan perustuva topologia

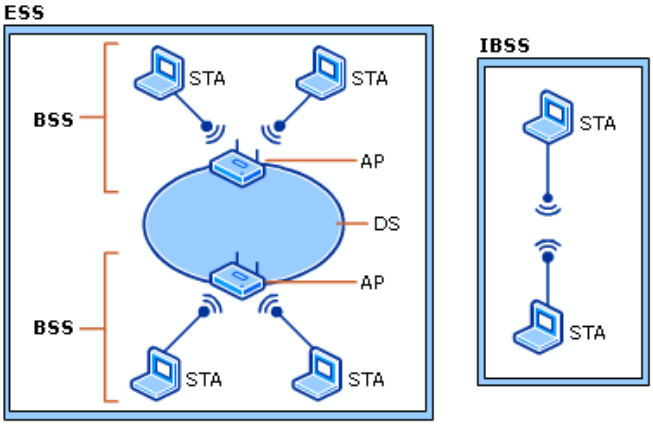
Yleisemmin käytetyssä, tukiasemaan perustuvassa BSS-topologiassa (Basic Service Set) eli niin sanotussa infrastruktuuriverkossa päätelaitteet liittyvät uuteen tukiasemaan, joka toimii yhdistävänä tekijänä runkoverkon ja langattoman verkon välillä (kuva 4). Verkossa olevien laitteiden välinen "keskustelu" kulkee tukiaseman kautta, joten BSS-verkon toimintaperiaate muistuttaa läheisesti kiinteiden lähiverkkojen toimintaa. (Granlund 2007, 294–295)



KUVA 4. Tukiasemaan perustuva verkkotopologia (wlan.com.br 2011).

Tukiasemaan perustuvaa BSS-verkkoa voidaan edelleen laajentaa, kun yksittäiseen BSS-tukiasemaverkkoon yhdistetään yksi tai useampia BSS-tukiasemaverkkoja, jotka kaikki käyttävät samaa runkoverkkoa. Tästä verkkoratkaisusta käytetään nimitystä ESS (Extended Service Set, kuva 5), jonka runkoverkko puolestaan on nimeltään DS (Distribution System). ESS-verkon avulla saadaan luotua vahvemmalla signaalilla toimivia ja laajemman peittoalueen kattavia langattomia lähiverkkoja. (Granlund 2007, 296.) Kun

langaton lähiverkko muodostuu useista limittäisistä ESS-verkoista, verkonkäyttäjä ei havaitse tukiasemanvaihdoksia eikä verkkoyhteys katkea siirryttäessä tiloista toiseen.

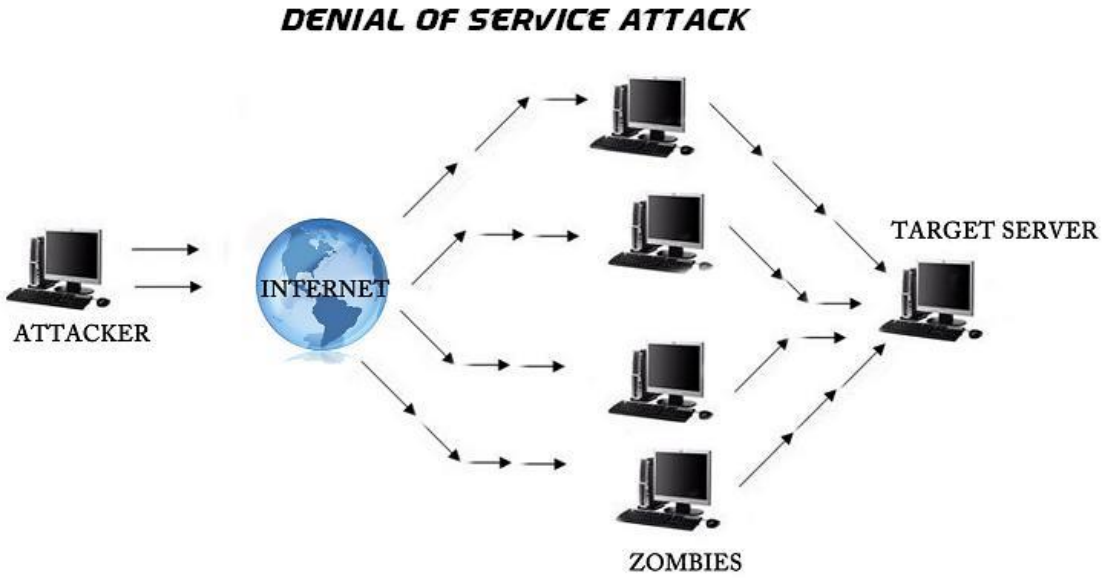


KUVA 5. Laajennettu tukiasemaan perustuva verkkotopologia (Jumpluf 2014).

2.3 Langattoman lähiverkon tietoturvauhat

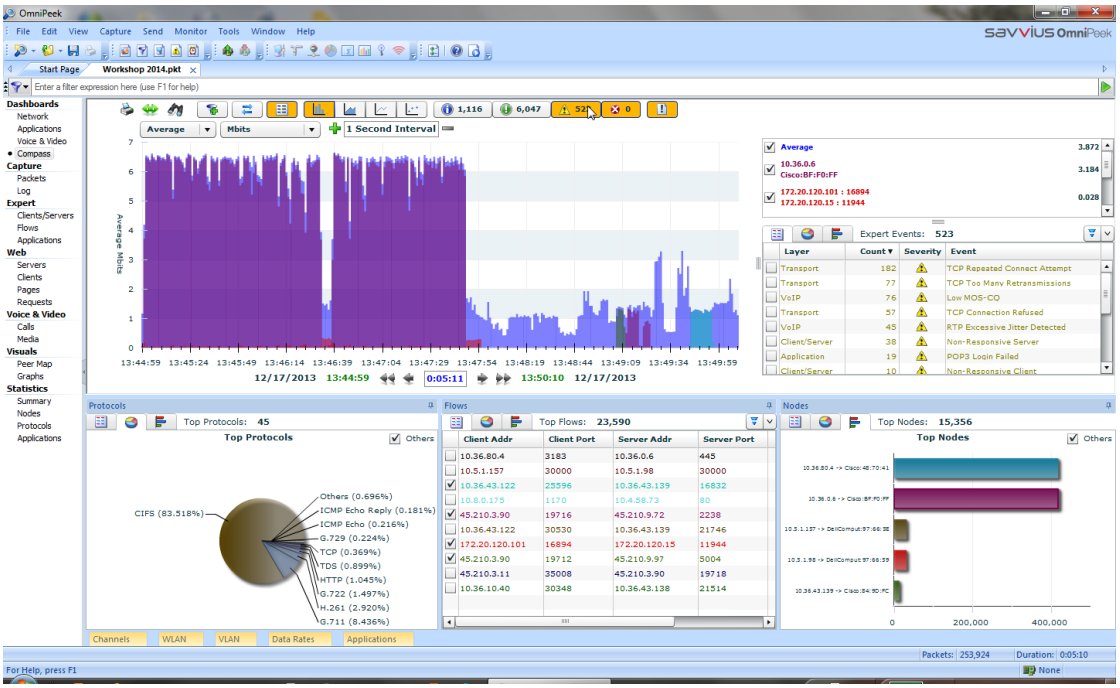
Langattomien lähiverkkojen tietoturvauhat ovat pääosin samoja kuin perinteisissä tietoverkoissa, mutta koska viestisignaalit etenevät WLAN-radioaalloilla ja ovat avoimesti käytettävissä, langattomuus mahdollistaa erilaisia murtautumismenetelmiä. Yritysten tuleekin olla tietoisia mahdollisista tietoturvauhista ja niiden torjumisesta. (Geier 2005, 171.)

Verkkoliikenteen vakavimpia uhkia ovat DoS- eli palvelunestohyökkäykset, joita kohdistetaan yleensä isoihin toimijoihin, kuten operaattoreihin ja pankkeihin. Palvelunestohyökkäys voidaan toteuttaa esimerkiksi niin sanottuna väsytyshyökkäyksenä, jossa verkkoon syötetään valtava määrä tietoa eli paketteja, kunnes verkon sietokyky ylittyy ja verkkoinfrastruktuurin toiminta keskeytyy aiheuttaen pahimmillaan laajoja käyttö- ja tietokatkoksia (kuva 6). Tällainen hyökkäys toteutetaan usein niin sanottuna hajautettuna palvelunestohyökkäyksenä (Distributed Denial of Service, DDoS), jolloin paketteja lähetetään esimerkiksi sähköpostipalvelimelle useiden kaapattujen tietokoneiden avulla. Palvelunestohyökkäyksiä vastaan voi varautua pitämällä yllä hyviä tietoturvakäytäntöjä esimerkiksi virustorjunnan, palomuurin ja vahvojen salasanojen osalta. (Geier 2005, 176–177.)



KUVA 6. DoS-palvelunestohyökkäyksen kaavio (Simard 2014).

Langattomien lähiverkkojen uhkana voidaan myös pitää verkkoliikenteen urkintaa ja analysointia. Verkon analysointia varten on saatavilla lukuisia siihen tarkoitettuja ohjelmia, joita voidaan käyttää myös salakuunteluun (kuva 7). Tietomurtautuja eli hakkeri voi päästä käsiksi pahimmillaan kaikkeen verkossa liikkuvaan tietoon aina käyttäjätunnuksista salasanoihin ja luottokorttinumeroista verkkopankkitunnuksiin.



KUVA 7. Ruudunkaappauskuva verkon vianmääritykseen ja analysointiin tarkoitetusta OmniPeek-ohjelmasta (Savvius 2015).

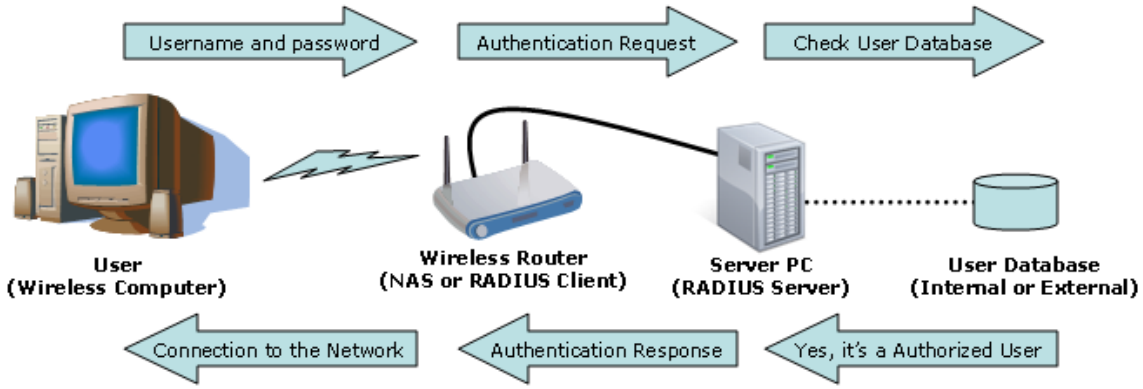
Edellä mainittujen tietoturvauhkien avulla tietomurtautujalla on yleensä tarve murtautua yrityksen sisäiseen tietojärjestelmään, kuten palvelimelle. Vaikka palvelinten tietoturvataso on useimmiten hyvä ja palvelimet ovat huolellisesti suojattuja, työasemien tietoturvapäivityksiä on voitu laiminlyödä, eikä niihin kohdistettuja hyökkäyksiä välttämättä heti havaita. Verkossa tapahtuvien väärinkäytösten estämiseksi suositellaan käytettävän suojattua https-yhteyttä internetsivuilla niin usein kuin mahdollista.

Langaton lähiverkkoyhteys tulisi myös olla suojattuna asianmukaisella tavalla. Mikäli muodostettu langaton lähiverkkoyhteys ei vaadi salausavaimia tai langattoman verkon tietoturvataso on heikko, suositellaan käytettävän VPN-yhteyttä, jolloin koko verkon liikenne on suojattu ja verkossa työskentely on turvallista. (Puska 2005, 69.) Seuraavassa kappaleessa käsitellään tarkemmin WLAN-verkon suojaamiseen liittyviä asioita.

2.4 Langattoman lähiverkon suojaaminen

IEEE 802.11-suosituksen mukaan langattoman lähiverkon tietoturvan tulee olla samalla tasolla kuin perinteistä kiinteää lähiverkkoa käytettäessä (Granlund 2007, 317). Langattomia lähiverkkoja – etenkin sen varhaisimpia standardeja – on kritisoitu huonosta tietoturvasta. Eräs langattoman verkon varhaisimmista salausmenetelmistä on symmetriseen salaukseen perustuva WEP (Wired Equivalent Privacy), joka julkaistiin vuonna 1997 samaan aikaan ensimmäisen 802.11-standardin kanssa. Vanhat verkkolaitteet tukevat edelleen WEP-salausta, joka käyttää salauksen purkamiseen aina samaa, selväkielistä avainta. WEP-salauksen saa murrettua siihen tarkoitetuilla ohjelmilla jopa alle minuutissa, joten kyseessä on tietoturvan kannalta erittäin haavoittuva ja puutteellinen salausmenetelmä. (Puska 2005, 47; Geier 2005, 178; Tietomurto.info 2008.)

WEP-salauksen tietoturvan heikosta tasosta johtuen IEEE korvasi sen turvallisemmalla WPA-salauksella (Wi-Fi Protected Access), joka julkaistiin vuonna 2003. WPA-salauksessa on käytössä kaksisuuntainen todennus, jossa laite ja verkko tunnistautuvat toisilleen esimerkiksi RADIUS-protokollan (Remote Authentication Dial-In User Service) avulla (kuva 8). (Geier 2005, 184–185.)



KUVA 8. Esimerkki RADIUS-palvelinta käyttävästä kaksisuuntaisesta todennuksesta, jossa käyttäjä tunnistetaan käyttäjätunnuksen ja salasanan avulla (Geier 2008).

Kaksisuuntaisen todennuksen lisäksi WPA-salaukseen sisältyy TKIP-mekanismi (Temporal Key Integrity Protocol), joka salaa jokaisen paketin uniikilla salausavaimella. TKIP:n avulla langattoman verkon turvallisuutta saatiin parannettua entisestään. (Geier 2005, 184–185.) Kaksi tietoturva-asiantuntijaa sai kuitenkin murrettua turvallisena ja varmana pidetyn WPA-salauksen vain 15 minuutissa (Pitkänen 2008).

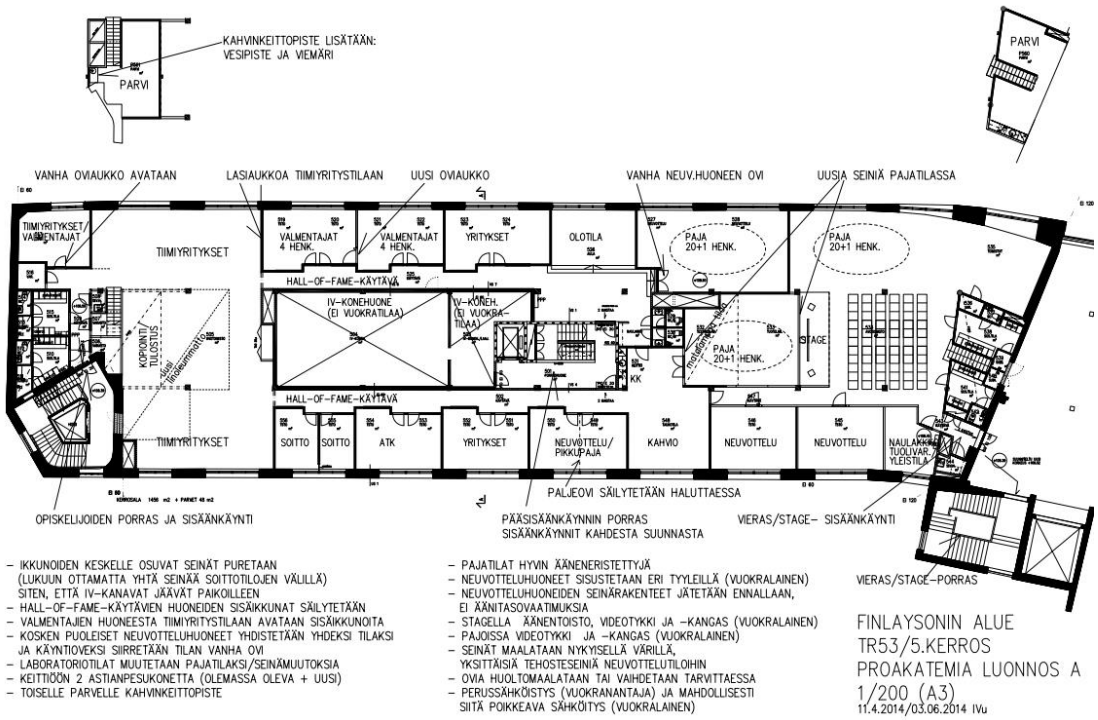
WPA-salauksen julkistamisen jälkeen IEEE perusti 802.11-verkon tietoturvaan keskittyvän työryhmän, WiFi-allianssin, joka julkaisi IEEE 802.11i-suosituksen eli WPA2-standardin vuonna 2004 (Granlund 2007, 317). WPA2-salauksen erittäin turvalliseksi tekee AES-lohkosalausmenetelmä, joka salaa ja purkaa tietoa useita kierroksia. AES-menetelmää pidetään murtamattomana ja se on yksi luotettavimmista salaustavoista. (Viljanen 2013–2015.)

Langattoman lähiverkon signaalia ei voida rajoittaa vain halutulle alueelle, vaan WLAN-radioaallot ja niiden sisältämä tieto ovat havaittavissa ja käytettävissä laajalla alueella ja esimerkiksi yritysten harmiksi myös yritystilojen ulkopuolella. Tiedon luottamuksellisuuden takaamiseksi on käytettävä salausta: esimerkiksi AES-, VPN- ja WPA2-salausmenetelmät tarjoavat asianmukaisen suojan turvalliseen tiedonsiirtoon langattomassa verkossa. (Puska 2005, 79.)

3 PROAKATEMIAN VERKKOYMPÄRISTÖ

3.1 Verkkoympäristön kartoitus

Proakatemian uusi kampus sijaitsee Finlaysonin alueella Tampereella. TR53 Värjäämönä tunnettu rakennus on valmistunut vuonna 1926. Vanha tehdasrakennus peruskorjattiin ja muutettiin toimistotiloiksi vuosina 2000-2001. (Finlaysonin alue 2015.) Proakatemian aiemmat toimitilat sijaitsivat myös Finlaysonin alueella, ja kuten edellisissä tiloissa myös uudella kampuksella on runsaasti vanhan tehdasrakennuksen suojeltuja elementtejä, kuten pylväitä, jotka ovat asettaneet raamit tilansuunnittelulle (kuva 9). Proakatemia siirtyi uusiin tiloihin kesällä 2015.



KUVA 9. Proakatemian uuden toimitilan pohjapiirros.

Proakatemian uusi toimitila on jaettu useisiin pienempiin opiskelijayritys-, valmennus- ja neuvottelutiloihin sekä muutamiin isompiin yhteistiloihin, kuten paja- ja kahvihuoneisiin. Koko Proakatemian toiminta sijaitsee TR53-rakennuksen 5. kerroksessa, joten verkkoympäristön näkökulmasta kyseessä on helposti toteutettava ja hallittava kokonaisuus. Proakatemian verkkoympäristö koostuu lukuisista eri aliverkoista: esimerkiksi henkilökunnan ja opiskelijoiden tietokoneille on omat aliverkkonsa.

Proakatemian verkkoympäristössä vierailevat käyttäjät pääsevät muodostamaan langattoman verkkoyhteyden joko TAMK-tunnuksilla tai manuaalisesti luotavilla käyttäjätunnus–salasana-yhdistelmillä. Verkkotunnuksia voidaan luoda tällä hetkellä joko Proakatemian päävalmentajan Veijo Hämäläisen tai TAMKin tietohallinnon IT-tuen toimesta. (Setälä 2015; TAMK 2013.)

3.2 Verkonkäyttäjien tarpeet ja vaatimukset

Yliopistot ja ammattikorkeakoulut, kuten myös Tampereen ammattikorkeakoulu, tarjoavat opiskelukäyttöön soveltuvat ammattimaiset tietotekniset laitteet ja apuvälineet. Yritysmaailmasta tuttu "bring your own device" eli BYOD-kulttuuri on kuitenkin tulossa myös oppilaitoksiin. BYOD-periaatetta suositaan etenkin IT-alan yrityksissä, joissa työntekijöiden ja heidän mukanaan kulkevien laitteiden tulee olla liikuteltavissa ja käytettävissä jouhevasti eri toimipaikkojen välillä. Kansainvälisen IT-alan tutkimus- ja konsultointiyrityksen Gartnerin mukaan 2010-luvun loppupuoliskolla jopa joka toinen työntekijä tekee töitä omalla tietokoneellaan (Olander 2015).

Proakatemian tilojen suunnittelussa on kiinnitetty huomiota BYOD-periaatteeseen, jotta työskentely kampuksella voisi olla mahdollisimman innovatiivista ja mieluisaa. Kannettavat ja tablettitietokoneet ovat korvanneet lähes täysin perinteiset pöytäkoneet, joten langattoman verkon kantavuuden ja toimintakyvyn tulee vastata muuttunutta työskentely-ympäristöä ja sen asettamia haasteita. Tietokoneiden lisäksi Proakatemian opiskelijat ja henkilökunta käyttävät muun muassa videoprojektoreita ja taulutelevisioita, joiden tulee olla toimintakykyisiä eri merkkisten ja mallisten laitteiden kanssa. (Mäkelä 2014).

3.3 Työasemat ja verkkolaitteet

Tampereen ammattikorkeakoulun tietohallinnon IT-erikoissuunnittelijan Sami Setälän (2015) mukaan Proakatemian tiloihin tulevien kiinteiden tietokoneiden lukumäärä on suhteellisen alhainen, mikä perustuu jo aiemmin hankittujen laitteiden runsaaseen määrään sekä BYOD-kulttuurin hiljattaiseen kasvamiseen. TAMKin työasemat ovat niin sanottuja leasing-tietokoneita, mikä tarkoittaa, että elinkaaren päässä olevat työasemat päivitetään uudempiin tietokoneisiin, eikä työasemien määrää ole täten tarvetta lisätä.

TAMKin opiskelijoita kannustetaan kuitenkin jo opintojen alkuvaiheessa hankkimaan oma kannettava tietokone, jota voi käyttää saumattomasti kodin ja oppilaitoksen välillä. TAMKin opiskelijat voivat asentaa joitain opiskeluun tarkoitettuja ohjelmia myös omille kotitietokoneilleen, kuten Microsoftin tunnetut toimisto-ohjelmat sisältävän Office ProPlus -ohjelmistopaketin.

Uusien tilojen käyttöönoton ja muuton yhteydessä Proakatemialla olevat pöytätietokoneet ja tulostimet kytkettiin kiinteään lähiverkkoon. Vaikka Proakatemian kampusalue sijaitsee Finlaysonin alueella Tampereen keskustassa, reitittimet, kytkimet ja muut verkkolaitteet sijaitsevat fyysisesti kolmen kilometrin päässä TAMKin Kuntokadun pääkampuksella Tampereen Kissanmaalla. Proakatemian uusi toimipaikka kytkettiin TAMKin runkoverkkoon, jotta Proakatemian verkkoa voidaan hallita keskitetysti TAMKin Kuntokadun kampukselta. (Setälä 2015; TAMK 2013.)

3.4 Langaton lähiverkko

Tampereen ammattikorkeakoulun kaikissa toimipisteissä on käytettävissä neljä erillistä langatonta verkkoa. Henkilökunnan käyttöön tarkoitettu TAMK-STAFF-verkko on rajattu toimimaan ainoastaan TAMKin työntekijöiden kannettavilla tietokoneilla. Opiskelijoiden ja vierailijoiden käytössä on TAMK-GUEST-verkko, jota voidaan käyttää joko TAMKin verkkotunnuksilla tai erikseen luotavilla väliaikaisilla vierailijatunnuksilla. Vierastunnuksia voivat tällä hetkellä luoda ainoastaan Proakatemian päävalmentaja Veijo Hämäläinen ja puhelimitse TAMKin tietohallinnon IT-tuki. (Setälä 2015; TAMK 2013.)

Käytössä on myös korkeakouluille suunnattu kansainvälinen Eduroam-verkko, jota voidaan käyttää kaikkien yhteistyökorkeakoulujen käyttäjätunnuksilla. Neljäntenä vaihtoehtona on Tampereen kaupungin ja ympäristökuntien muodostaman Langattoman Tampereen LANGATON-WPA-verkon käyttäminen, johon pääsee kirjautumaan myös TAMKin henkilökunnan ja opiskelijoiden tunnuksilla.

Tampereen ammattikorkeakoulun IT-erikoissuunnittelijan Sami Setälän (2015) mukaan TAMKin tietohallinnon kehityshankkeena on kaikissa korkeakoulun toimitiloissa toimiva ja kaikille käyttäjille avoin vierasverkko. Tämän myötä kuka tahansa pääsisi käyt-

tämään verkkoyhteyttä hyväksymällä TAMKin tietohallinnon asettamat käyttöehdot ja noudattamalla tietoturvalakia. Tällaisen verkkokokonaisuuden toteuttaminen vaatii kuitenkin lisäresursseja, jotta verkkoon kohdistuvat väärinkäytösyritykset saadaan estettyä, joten verkkoprojektin toteuttamisen tarkemmat aikataulut ja yksityiskohdat tarkentunevat lähitulevaisuudessa. (Setälä 2015.)

Proakatemian kampuksen ja muidenkin TAMKin toimipisteiden langaton lähiverkko on toteutettu niin sanottujen WLAN-kontrollerien ja -moduulien avulla. Tämä tarkoittaa käytännössä sitä, että verkossa on yksi itsenäinen hallinta- eli kontrollerilaite, jolla voidaan ohjata tukiasemien toimintaa. Kontrolleripohjaisen verkon myötä kaikkien toimipisteiden langattomat verkkopalvelut ovat identtiset ja TAMKin tietohallinto voi hallita niitä keskitetysti. Kontrolleripohjaisen verkon etuna on myös sen skaalautuvuus, eli langattoman lähiverkon toimintakykyä voidaan parantaa yksinkertaisesti lisäämällä ylimääräisiä tukiasemia verkkokontrollerin hallittavaksi. (Setälä 2015.)

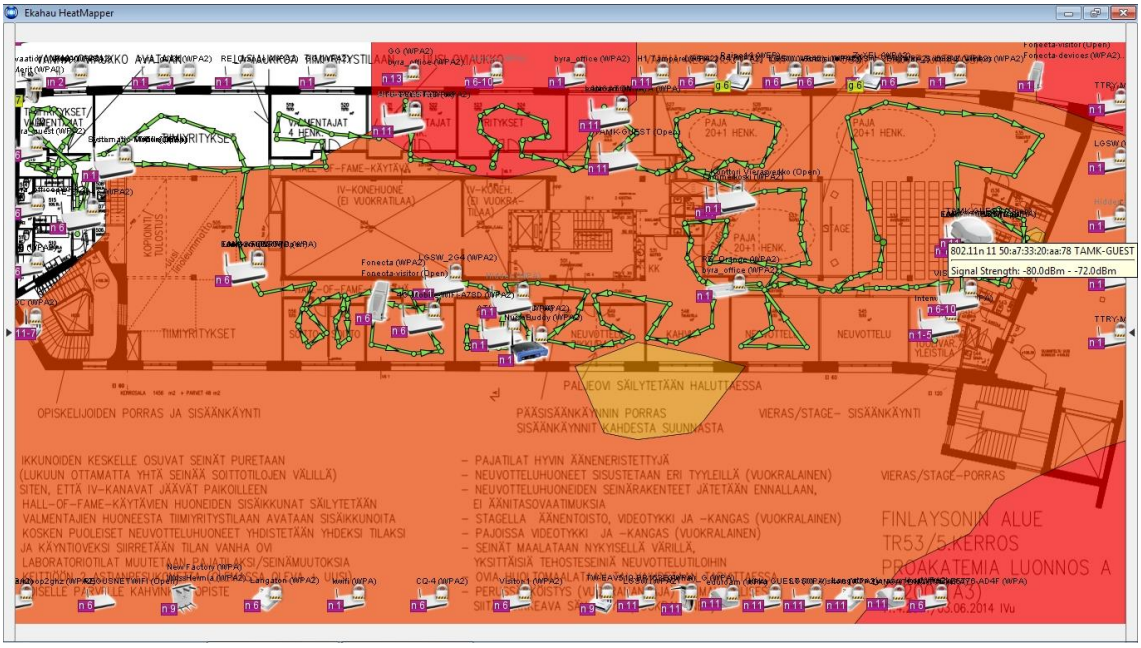
Proakatemian toimitiloissa on kolme yhdysvaltalaisen Ruckus-valmistajan ZoneFlex R600 -tukiasemaa (kuva 10) eri puolella kampusta. Kyseessä on 802.11ac-standardin mukainen MIMO-tekniikkaa tukeva tukiasema sisäkäyttöön. Tukiasema mahdollistaa verkon jakamisen yhtäaikaisesti jopa 500 käyttäjälle. Sen vuoksi ZoneFlex R600 -tukiasema sopii nimenomaan kouluihin ja oppilaitoksiin. (Daimler 2010.)

KUVA 10. Ruckus ZoneFlex R600 -tukiasema (Ruckus 2015).

4 LANGATTOMAN LÄHIVERKON KANTAVUUDEN MITTAAMINEN

4.1 Mittauksen lähtökohdat

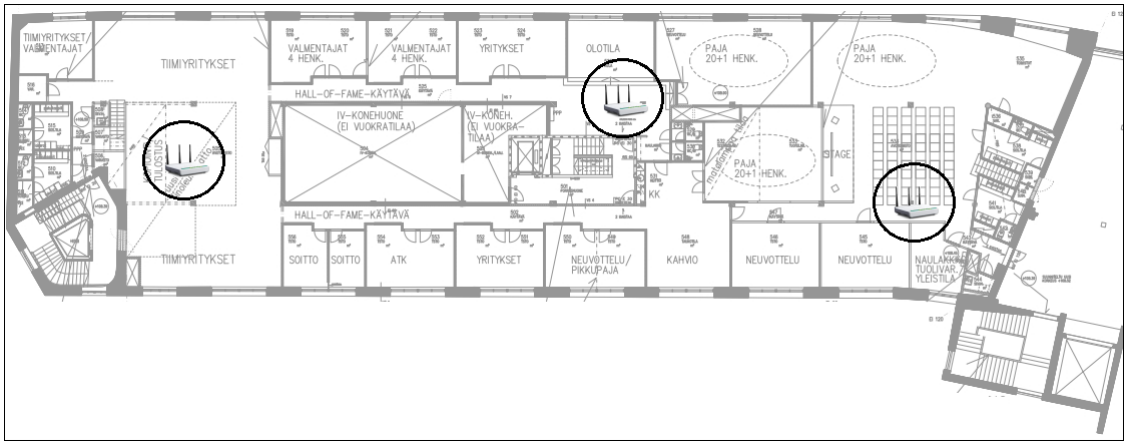
Tämän opinnäytetyön yhtenä päätarkoituksena oli mitata ja tutkia langattoman lähiverkon toimivuutta Proakatemian uusissa toimitiloissa. Proakatemian kampus on vanhan tehdasrakennuksen ylimmässä kerroksessa. Sen lisäksi rakennuksessa toimii lukuisia muita yrityksiä ja niiden toimistotiloja. Muiden yritysten langattomat verkot näkyvät ja kuuluvat myös langattomien verkkojen radioaalloilla (kuva 11), mikä asettaa haasteita myös Proakatemian langattoman verkon toiminnalle. Proakatemian kampuksen verkonmittaus tehtiin elokuussa 2015 Ekahau HeatMapper -mittausohjelman avulla. Verkon mittaus tehtiin itsenäisesti omien ja Proakatemian aikataulujen puitteissa. Apuvälineenä käytettiin henkilökohtaista kannettavaa tietokonetta, jonka avulla koko verkko mitattiin yhdellä kerralla, joten mittauksesta saadut tulokset ovat suuntaa antavia.



KUVA 11. Langattoman lähiverkon mittaukseen tarkoitettu Ekahau HeatMapper -ohjelma havaitsee kymmeniä ulkopuolisten verkkojen tukipisteitä Proakatemian tiloissa. Ruudunkaappauskuva Ekahau HeatMapper -ohjelmasta.

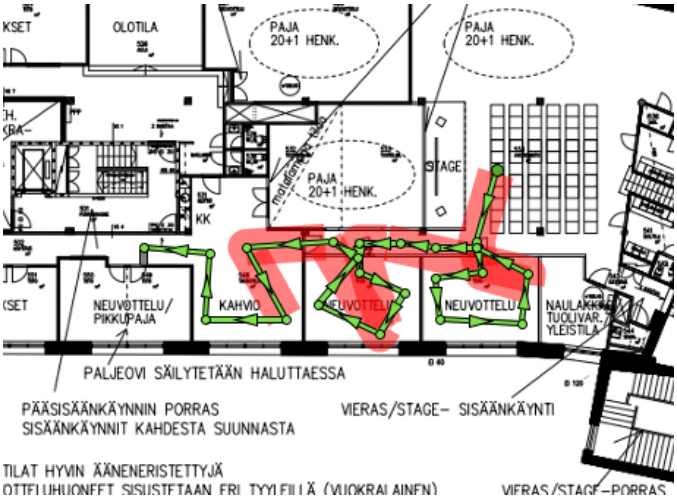
TAMKin tietohallinnon työryhmä on tehnyt IT-erikoissuunnittelijan Sami Setälän (2015) mukaan alustavia WLAN-verkon mittauksia Proakatemian uusissa tiloissa, mutta toistaiseksi tukiasemat on sijoiteltu tilapäisiin paikkoihin alkusyksyllä 2015 meneillään

olleen remontin vuoksi (kuva 12). Tämän tutkimuksen puitteissa suoritettiin erillinen lähiverkkojen kartoitusmittaus, jonka tuloksia käsitellään seuraavassa luvussa.



KUVA 12. Kolmen tukiaseman sijoittelu Proakatemian kampuksella ennen tämän tutkimuksen mittauksia.

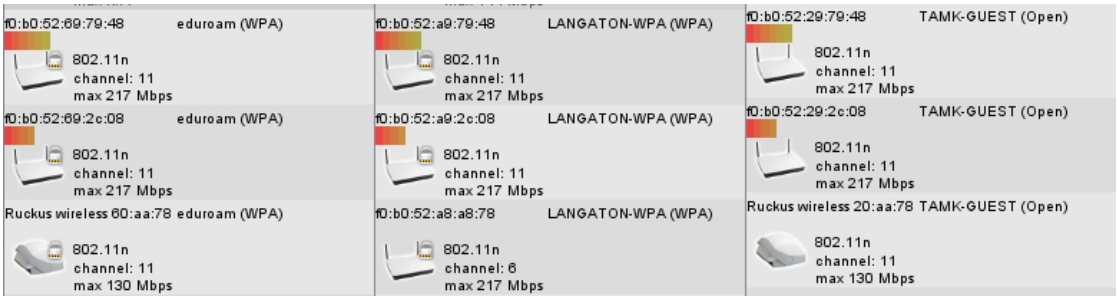
Proakatemian langatonta verkkoa kartoitettaessa käytettiin Sonyn Vaio VPCEH1L0E -kannettavaa tietokonetta ja langattoman verkon mittaukseen soveltuvaa Ekahau HeatMapper -ohjelmaa. Kyseessä on suomalaisen ohjelmistoyrityksen Ekahaun yksinkertaistettu ilmaisversio yrityskäyttöön tarkoitetusta Ekahau Site Survey -ohjelmasta. Ohjelman lataamisen ja asennuksen jälkeen ohjelmaan avataan halutun tilan pohjakartta, jonka jälkeen tietokoneen kanssa kuljetaan mittausalueen läpi klikkaamalla hiirtä eri puolella mittausaluetta (kuva 13). Mittauksen päätyttyä HeatMapper-ohjelma kartoittaa langattomat verkot ja tukiasemat pohjapiirrokseen lämpökarttakuvana, jossa vihreä tarkoittaa vahvaa, keltainen keskinkertaista ja punainen heikkoa kuuluvuutta.



KUVA 13. Ekahau HeatMapper -ohjelmassa mitataan halutun tilan langattoman verkon kuuluvuus klikkaamalla sijaintia kartalla. Ruudunkaappauskuva.

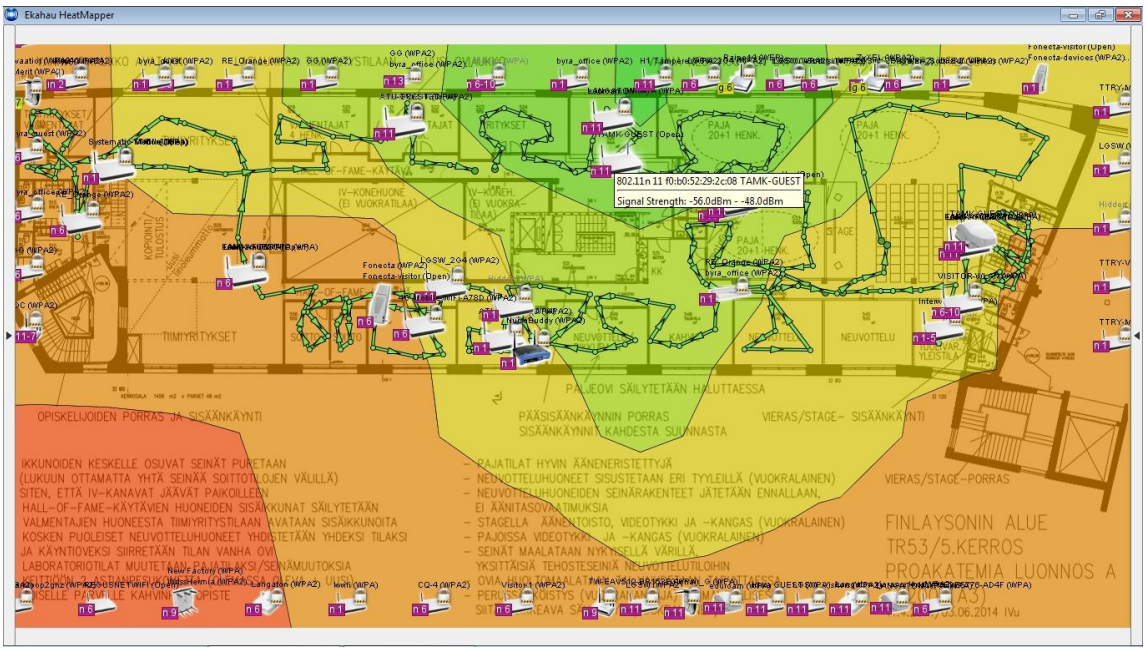
4.2 Mittaustulokset ja niiden analysointi

Langattomien lähiverkkojen mittaus tehtiin TAMK-GUEST-verkkoon kirjautuneena. Proakatemian langattomien verkkojen toiminta on kolmen tukiaseman varassa (kuva 14). Nämä tukiasemat takaavat Eduroam-, LANGATON-WPA-, TAMK-GUEST-ja TAMK-STAFF-verkkojen toiminnan.

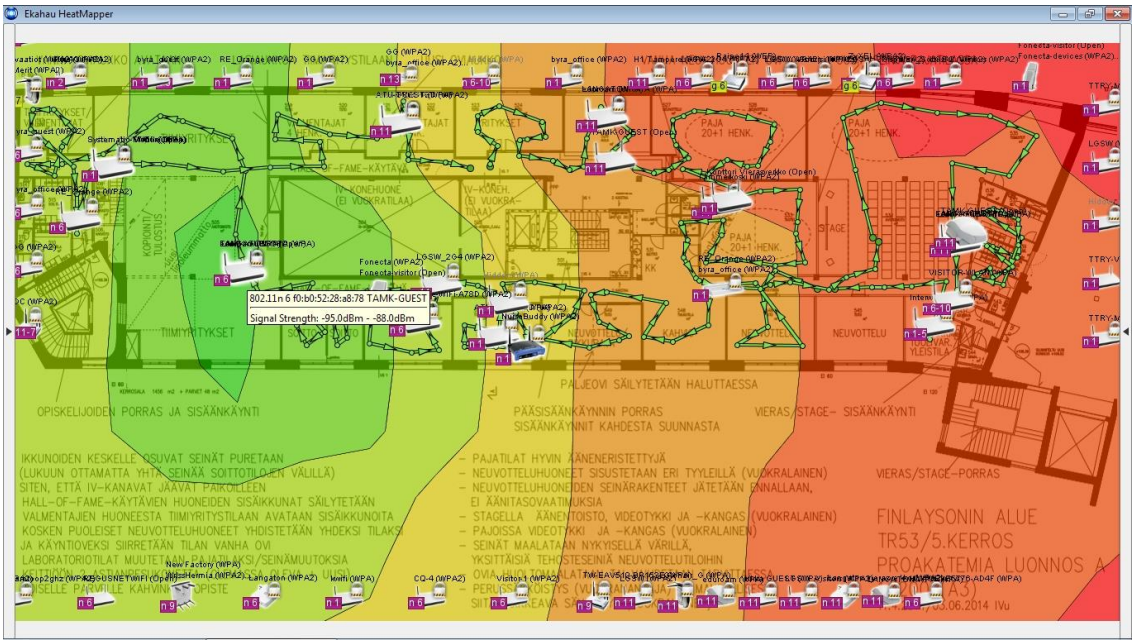


KUVA 14. Proakatemian langattomat lähiverkot sekä niiden salaustyypit, standardit, kanavat ja teoreettiset maksiminopeudet. Ruudunkaappauskuva Ekahau HeatMapper -mittausohjelmasta.

Proakatemian tiloissa aiemmin toimineen tietoturvayrityksen jäljiltä joidenkin seinien rakenteissa on metallilevyjä, jotka vaimentavat verkkosignaalin kantavuutta ja kuuluvuutta (Hämäläinen 2015). Mittaustuloksissa nämä metallilevyin eristetyt tilat eivät kuitenkaan erottuneet, joten käytännössä niiden vaikutus on melko vähäinen. Mittausten perusteella Proakatemian toimitilan keskelle sijoitettu tukiasema kattaa suuren osan kampustilasta (kuva 15). Heikoimmat kuuluvuusalueet sijaitsevat tilan länsiosassa Proakatemian tiimiyritysten tilojen kohdalla sekä mahdollisesti aivan rakennuksen itäpäässä olevassa kahvihuoneessa.



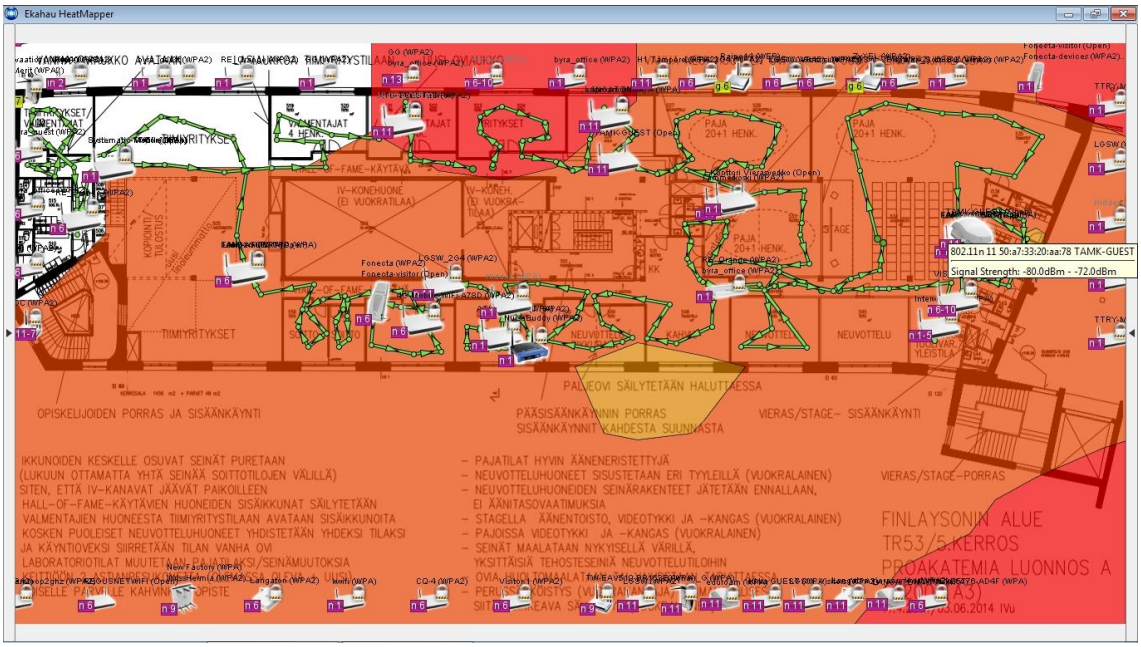
KUVA 15. Keskimmäisen tukiaseman kantavuus TAMK-GUEST-verkkoa mitattaessa. Ruudunkaappauskuva Ekahau HeatMapper -mittausohjelmasta.



KUVA 16. Toimitilan länsisiivessä olevan tukiaseman kantavuus TAMK-GUEST-verkkoa mitattaessa. Ruudunkaappauskuva Ekahau HeatMapper -mittausohjelmasta.

Kuten yläpuolella olevasta kuvasta (kuva 16) käy ilmi, toisen tukiaseman peittoalue kattaa rakennuksen länsipuolen katvealueet. Kun tarkastellaan molempien tukiasemien peittoalueita, voidaan todeta, että Proakatemian tärkeimmät tilat, kuten kokous- ja tiimitilat, ovat hyvän verkkokuuluvuuden piirissä. Ainoastaan toimipisteen itäsiivessä olevan auditoriotilan kuuluvuus jää keskinkertaisen kuuluvuuden alueelle. Auditoriotilassa lan-

gattoman verkon kuuluvuuden tulisi olla ehdottomasti parempi tilan korkean käyttöasteen vuoksi. Kolmas tukiasema sijaitsee kampuksen itäpäädyssä suuren pajatilan ja lavan lähettyvillä. Kyseisen tukiaseman toiminta oli ainakin mittaushetkellä epäilyttävän heikko (kuva 17), mikä johtunee tukiaseman tilapäisestä sijoituspaikasta.



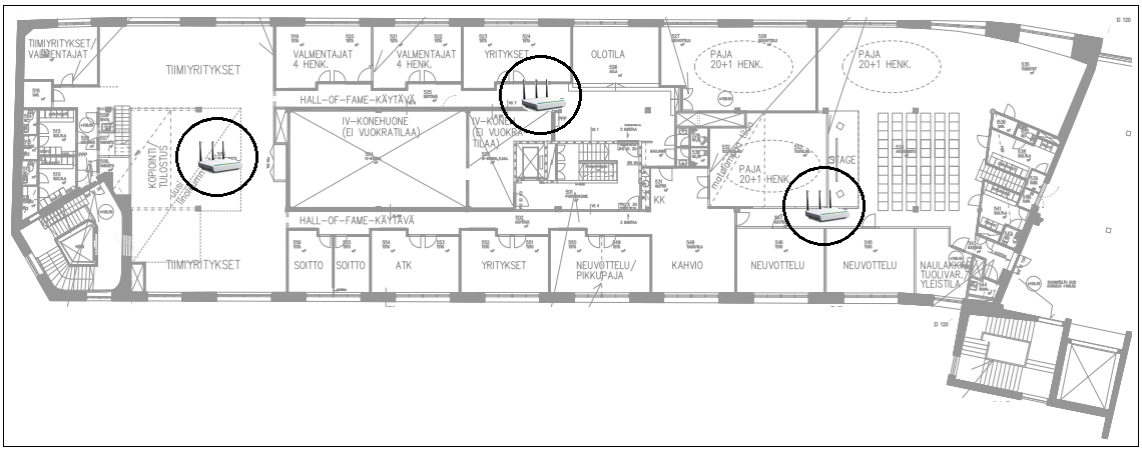
KUVA 17. Itäsiivessä olevan tukiaseman kantavuus TAMK-GUEST-verkkoa mitattaessa. Ruudunkaappauskuva Ekahau HeatMapper -mittausohjelmasta.

4.3 Parannusehdotukset

Langattoman verkon kuuluvuuden parantamiseksi tilojen keskiosassa olevaa tukiasemaa voisi siirtää lähemmäksi auditoriotilaa ja toisen tukiaseman sijaintia hieman keskemmälle Proakatemian kampusta (kuva 18). Täten taataan sekä hyvä langattoman verkon peittoalue Proakatemian toimitiloissa että vahva signaali kampuksen tärkeimmissä tiloissa. Tilojen pohjoissiivessä sijaitsevissa valmentajien huoneissa käytetään lähinnä pöytätietokoneita, joten langattoman verkon vahva kuuluvuus näissä tiloissa ei ole välttämätöntä.

Kuvassa 18 osoitetun tukiasemien uudelleensijoittelun myötä myös WLAN-verkon kuuluvuus täytyy kartoittaa eli mitata uudelleen. Uudet mittaustulokset osoittanevat verkon vahvemman kuuluvuuden sen vaatimissa tiloissa. Uusien mittausten suunnittelua ja to-

teuttamista sekä mittaustulosten tutkimista ei sisällytetty tähän opinnäytetyöhön aikataulullisista syistä.



KUVA 18. Hahmotelma tukiasemien uudelleensijoittelusta.

5 YHTEENVETO

Langattoman lähiverkon nopeus, turvallisuus ja luotettavuus ovat nykyään sillä tasolla, että langattoman verkon käyttöä voidaan pitää luotettavana vaihtoehtona sekä yksityis- että yrityskäytössä. Uusien tekniikoiden myötä tiedonsiirtonopeudet kasvanevat vielä entisestään. Proakatemian uuden kampusrakennuksen tukiasemien tämänhetkinen määrä ja niiden sijoittelu takaa hyvän langattoman lähiverkon peittoalueen miltei joka puolella Proakatemian toimipistettä.

Langattoman verkon kantavuutta ja kuuluvuutta mitattaessa havaittiin, että tilojen välillä ei ole suuria eroavaisuuksia kuuluvuudessa, mikä on tärkeää langattoman verkon käyttäjälle. Kartoitustutkimuksessa langattoman verkon peittoalueessa ei ollut suuria puutteita, mutta parannusehdotuksia löytyi ja niitä tuotiin esille langattoman lähiverkon mittaamista käsittelevässä alaluvussa 4.3. TAMKin IT-erikoissuunnittelijan Sami Setälän (2015) mukaan Proakatemian uusissa toimitiloissa on tehty alustavia verkonmittauksia, mutta niitä ei ole vielä hyödynnetty tukiasemien sijoittelun ja täten langattoman lähiverkon toimivuuden parantamisessa. Tässä tutkimuksessa saadut mittaustulokset luovutetaan TAMKin tietohallinnolle, joka tulee tekemään tukiasemien uudelleensijoittelua loppuvuonna 2015.

Opinnäytetyön myötä opin langattoman verkon suunnittelusta ja mittauksesta todella paljon uutta. Verkonmittaukseen soveltuvia ohjelmia on runsaasti tarjolla, ja opinnäytetyöhön valittu HeatMapper osoittautui sekä helppokäyttöiseksi että luotettavaksi vaihtoehdoksi. Lisäksi tutustuin langattomien lähiverkkojen tekniikoihin ja tietoturvaan aiheeseen liittyvien kirjallisuuden ja verkkolähteiden avulla. Sain tutkimuksen kirjoittamiseen konsultointiapua Proakatemian päävalmentajalta Veijo Hämäläiseltä, TAMKin IT-erikoissuunnittelijalta Sami Setälältä sekä TAMKin ICT-päälliköltä Mikko Mäkelältä.

LÄHTEET

Ahonen, V. 2014. IEEE 802.11. Luettu 19.8.2015. http://spacebimbom.com/kategoriat/tiede/ieee-80211.php

Computer History Museum. 2015. Luettu 14.10.2015. http://archive.computerhistory.org/resources/access/physical-object/2009/04/102711359.01.01.lg.JPG

Daimler. 2010. Luettu 10.9.2015. http://www.daimler.fi/tuotteet/langattomat-verkot/wlan-verkot/ruckus-wireless/tuotteet/tukiasemat/zoneflex-r600

Geier, E. 2008. Luettu 19.8.2015. http://www.wi-fiplanet.com/img/2008/08/Tutorial%20-%20Geier%20E%20-%201051%20-%20Figure%201.png

Geier, J. 2005. Langattomat verkot perusteet. Helsinki: IT Press.

Granlund, K. 2007. Tietoliikenne. 1. painos. Jyväskylä. WSOYpro/Docendo.

Hämäläinen, V. Päävalmentaja. 2015. Henkilökohtainen tapaaminen 30.3.2015.

Finlaysonin alue. 2015. TR53 Värjäämö. Luettu 20.8.2015. http://www.finlaysoninalue.fi/historiaa_1820-/rakennukset/varjaamo

Jumpluff, K. 2014. Luettu 20.8.2015. http://community.arubanetworks.com/t5/image/serverpage/image-id/12838i6135E43350D638A9/image-size/original?v=mpbl-1&px=-1

Jumpluff, K. 2014. Luettu 20.8.2015. http://community.arubanetworks.com/t5/image/serverpage/image-id/12840iE09581167A12D3A4/image-size/original?v=mpbl-1&px=-1

Järvinen, P. 2002. Tietoturva & yksityisyys. 2. painos. Jyväskylä: Docendo Finland Oy.

Kelly, V. 2014. New IEEE 802.11ac™ Specification Driven by Evolving Market Need for Higher, Multi-User Throughput in Wireless LANs. Luettu 26.8.2015. http://standards.ieee.org/news/2014/ieee_802_11ac_ballot.html

Lammle, T. 2010. CCNA wireless study guide (IUWNE 640-721). Wiley Technology Pub.

Mäkelä, M. 2014. Henkilökohtainen sähköpostikeskustelu 27.10.2014.

Mäkinen, S. 2012. Uusi standardi tuo Gigabit-nopeudet WLAN-verkkoon. Luettu 6.9.2015. http://www.nylund.fi/fi/yritys/ajankohtaista/asiantuntija-artikkeleita/uusi-standardi-tuo-gigabit-nopeudet-wlan-verkkoon.html#.VPnNPzSsVMc

Olander, I. 2015. BYOD eli kuluttajistuminen oppimisessa ja työssä. Luettu 10.9.2015. http://sometek.fi/byod-eli-kuluttajistuminen-oppimisessa-ja-tyossa

Pitkänen, P. 2008. Wlan-salaus murrettiin. Luettu 29.9.2015. http://www.digitoday.fi/tietoturva/2008/11/06/wlan-salaus-murrettiin/200828904/66

Pohjonen, R. 2002. Tietojärjestelmien kehittäminen. 2. painos. Jyväskylä: Docendo.

Proakatemia. 2015. Luettu 19.8.2015. http://www.proakatemia.fi

Puska, M. 2005. Langattomat lähiverkot. Helsinki: Talentum.

Puustinen, J. 2009. Tietoviikko: Uusi wlan-standardi hyväksytty - nopeudet jopa 600 Mbit/s. Luettu 26.8.2015. http://www.tivi.fi/Uutiset/2009-09-12/Uusi-wlan-standardi-hyv%C3%A4ksytty---nopeudet-jopa-600-Mbits-3175073.html

Ruckus.com. 2015. Luettu 6.9.2015. http://6915416c32e4851eca5d-c094c6710edd9b0999733b05a7cec13d.r9.cf2.rackcdn.com/images/products/r600.png

Savvius.com. 2015. Luettu 6.9.2015.https://www.savvius.com/images/screenshots/omnipeek_compass_lg.png

Setälä, S. 2015. Henkilökohtainen sähköpostikeskustelu 1.9.2015 ja 9.9.2015.

Shimpi, A. 2012. 5th Generation WiFi: 802.11ac, "Gigabit" WiFi Primer. Luettu 10.9.2015.http://images.anandtech.com/doci/5292/Screen%20Shot%202012-01-05%20at%2012.03.48%20AM.png

Simard, E. 2014. Protecting Your DNS Server Against DDoS Attacks. Luettu 6.9.2015. http://www.gtcomm.net/blog/wp-content/uploads/2014/02/dos-attack-schema.jpg

TAMK. 2013. Luettu 29.9.2015. https://intra.tamk.fi/web/it-ohjeet/langaton-verkko

Tietomurto.info. 2008. Langattoman verkon ja tukiaseman suojaaminen. Luettu 19.8.2015. http://www.tietomurto.info/artikkelit/WPA-suojaus_ja_WLAN-asetukset.php

Viljanen, V. 2013-2015. Luettu 19.8.2015. Tietojen salaaminen. https://www.yksityisyydensuoja.fi/tietojen-salaaminen

Wlan.com.br. 2011. Luettu 20.8.2015. http://www.wlan.com.br/wp-content/gallery/topologia-802-11/bss_picture.png